Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1

ISACA®
Barcelona Chapter

I Jornada Tecnològica

Riscos a considerar en l'ús de la tecnologia per part de l'auditor

Joaquim Altafaja

Què és ISACA?

ISACA
Barcelona Chapter

- ✓ **ISACA** **I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation (Associació pel Control i l'Auditoria dels Sistemes d'Informació). Establerta als EEUU al 1969.

- ✓ És una associació professional sense ànim de guany. El conjunt de membres de l'associació forma una organització de voluntaris al servei de la governança de les Tecnologies de la informació.

Capítols al món

ISACA Barcelona Chapter

Arribem als 215 Capítols!

Capítols a 92 països, 6 continents

Associats a 187 països

Junts, arribem a més de 140.000 membres

ISACA
Trust in, and value from, information systems
215 CHAPTERS STRONG

Missió ISACA

ISACA Barcelona Chapter

- ✓ La nostra missió és proporcionar coneixement, certificacions, formació en auditoria, seguretat i govern de sistemes i tecnologies de la informació, així com els riscos i compliment relacionats amb les TIC.

- ✓ Oferim recolzament als empresaris, auditors, universitats, administració pública, així com donem suport a l'administració pública catalana i als òrgans judicials i de l'advocacia en l'àmbit de les TIC.

- ✓ **ISACA** ajuda a les empreses i caps de TI a construir la confiança i seguretat en els sistemes d'informació.


VIII CONGRÉS ISACA BARCELONA
(Sec + Priv)gov = Ús ètic de la tecnologia
50 ISACA
HONORING OUR PAST.
INNOVATING OUR FUTURE.
29 Octubre de 2019
En el marc de:
Fira Barcelona
BARCELONA
CYBERSECURITY
CONGRESS

Riscos a considerar en l'ús de la tecnologia per part de l'auditor

ISACA Barcelona Chapter

Auditor  Tecnologia

Auditoria ⟷ Tecnologia

ISACA
Barcelona Chapter

Auditor ⟷ Tecnologia

ISACA
Sistemas de información fiables y valiosos
Barcelona Chapter

Material de referencia y ayuda a la norma técnica de auditoría de cuentas en entornos informatizados, BOICAC 54

Con el soporte institucional de

COL·LEGI DE CENSORS JURATS DE COMPTES DE CATALUNYA

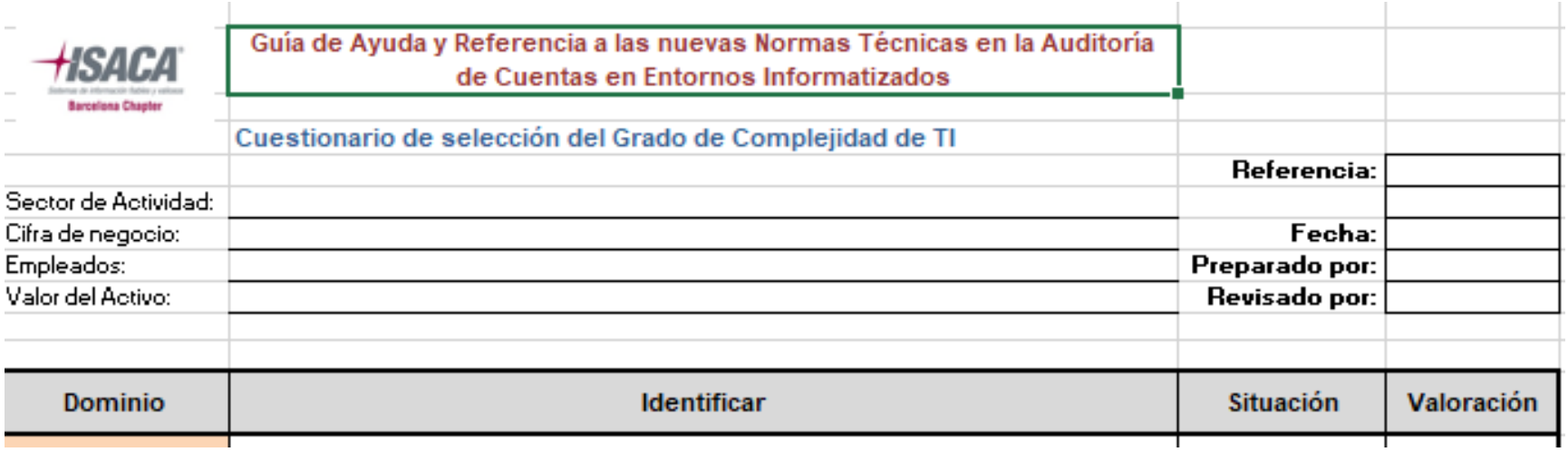
economistas

07/06/2011

Auditor ⟷ Tecnologia

Presentación de la Guía de Ayuda y Referencia a las nuevas Normas Técnicas en la Auditoría de Cuentas en Entornos Informatizados

03/06/2013



Guía de Ayuda y Referencia a las nuevas Normas Técnicas en la Auditoría de Cuentas en Entornos Informatizados

Cuestionario de selección del Grado de Complejidad de TI

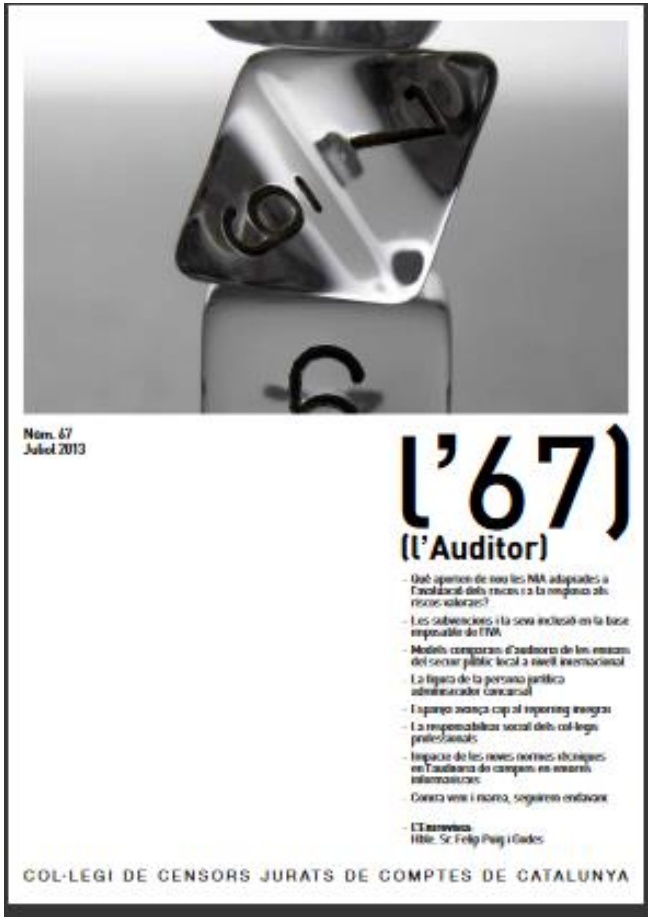
		Referencia:	
Sector de Actividad:			
Cifra de negocio:		**Fecha:**	
Empleados:		**Preparado por:**	
Valor del Activo:		**Revisado por:**	

Dominio	Identificar	Situación	Valoración

Auditor ⟷ Tecnologia

Modelo del grado de complejidad de TI	Bajo	Medio	Alto
Servidores (Estructura)	1	2 - 3	> 3
Sistemas Operativos (Estructura)	Estándares	No estándares o más de 1	Múltiples o WAN
Estaciones de Trabajo (Estructura)	1 – 15	15 – 30	> 30
Puestos de trabajo remotos (Organización)	Ninguno	1 – 2	> 2
Aplicaciones Informáticas (Aplicaciones)	Estándar de mercado	Estándar adaptado	Sistemas integrados ERP
Aplicaciones informáticas que realizan cálculos automáticos de cierta complejidad (Aplicaciones)	Ninguno	1 - 2	> 2
Aplicaciones informáticas desarrolladas internamente por la compañía (Aplicaciones)	Ninguno	1 - 2	> 2
Número de interfaces entre aplicaciones informáticas (Aplicaciones)	0 - 1	2 - 3	> 4
Control interno sobre los informes financieros (Aplicaciones)	Informes estándares	Informes estándares y algunos a medida	Informes desarrollados a medida
Procesos avanzados de TI (Complejidad)	Ninguno a Pocos	Pocos a Moderados	Moderados a Muchos
Transacciones economicas en línea (Complejidad)	No	Pocas	Muchas

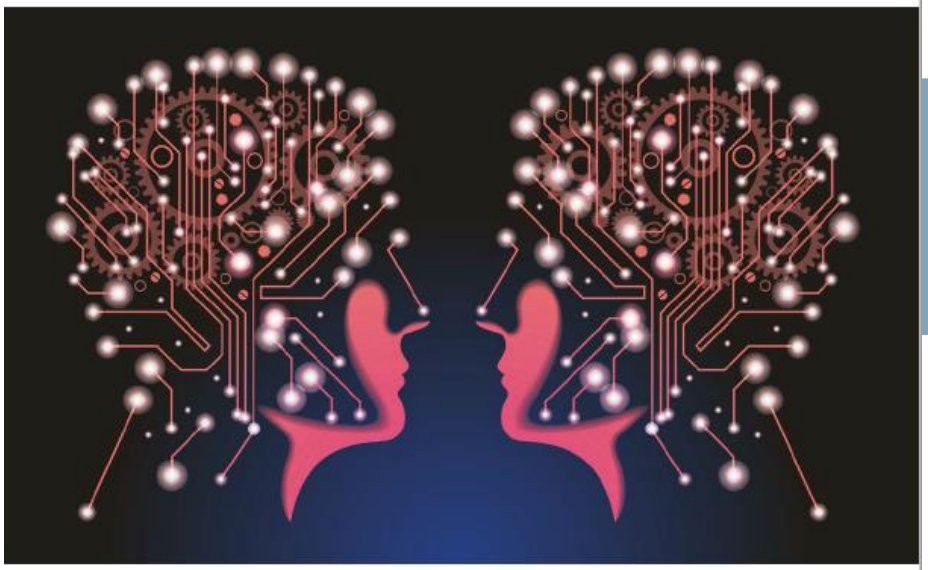
Auditor ⟷ Tecnologia



ISACA
Barcelona Chapter

Auditor ⟷ Tecnologia

l'Auditor) 79



Núm. 79
Juliol 2017

Preparats ja per al canvi en els informes d'auditoria

Entendre i auditar els nous models de negoci

l'auditoria)

La ciberseguretat, un nou component de risc rellevant en l'auditoria de comptes

Joaquim Altafaja Diví

L'última quinzena de maig ha estat especialment convulsa pel que fa als sistemes d'informació. Si el ramsonware, virus "extorsionador" com l'anomenen alguns, Wanna Cry, va causar estralls en l'àmbit mundial, ja que va infectar més de 360.000 ordinadors en 180 països, i es va confirmar un impacte en les infraestructures crítiques espanyoles d'almenys una desena d'aquestes, l'últim cap de setmana de maig, l'apagada accidental del sistema informàtic de la companyia aèria British Airways va provocar el caos en els dos aeroports més grans de Londres, ja que van deixar 75.000 passatgers a terra i un embolic de maletes mundial.

Riscos a considerar en l'ús de la tecnologia per part de l'auditor

ISACA Barcelona Chapter

Auditor ⟷ Tecnologia

ISACA
Barcelona Chapter

Auditor  Tecnologia

L'Auditor te "Arte y Parte"

ISACA Barcelona Chapter

Conèixer la entitat i el seu entorn

1. Coneixement de l'entorn

2. Control intern (basat en COSO)
   a. Coneixement de l'entorn general
   b. Procés de valoració dels riscos per la entitat
   c. Sistemes d'informació
   d. Activitats de control rellevants
   e. Seguiment

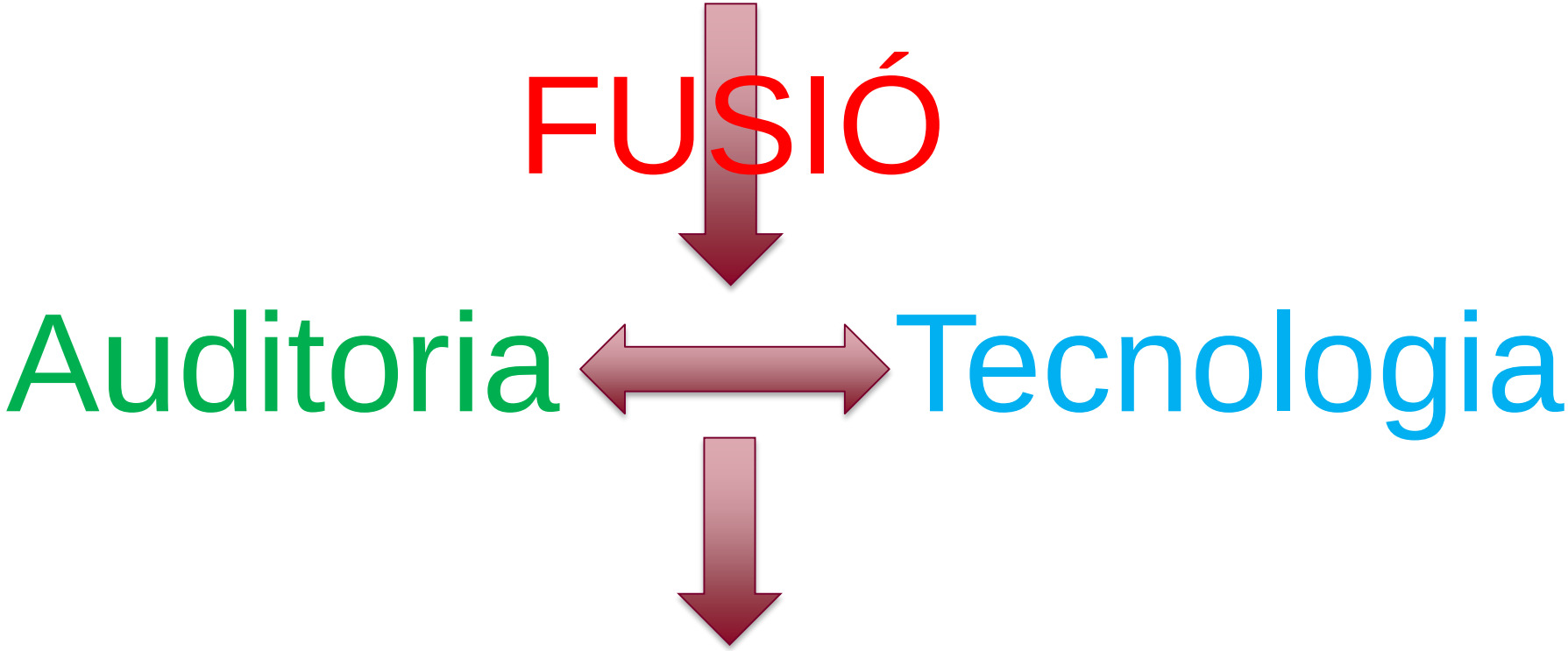
Parte

ISACA Barcelona Chapter

Avui la TECNOLOGIA, està a l'epicentre de les idees i de l'acció o govern, que al seu torn proveeix i es retroalimenta en l'actual món digital mitjançant l'estratègia i els projectes, amenaçats pels riscos, i tot això, en aquest context social de híper connexió de les persones, en una nova societat on la frontera entre el personal i el professional, el públic i el privat, el tangible i l'eteri, es dilueixen al voltant de les tecnologies de la informació

Nosotros, los auditores, estamos en una senda donde es necesario evolucionar, no solo porque nuestros clientes lo están haciendo, sino porque la profesión, ha emprendido un camino sin retorno. Las nuevas capacidades solicitadas en nuestros profesionales, la generación de oportunidades para el talento así como las nuevas formas de trabajar con herramientas y tecnologías a disposición de las firmas, son factores clave para el futuro de la profesión (Loreta Calero – Presidenta CIT)

Futur immediat



LA TRANSFORMACIÓN DIGITAL EN EL SECTOR DE LA AUDITORÍA

CONCLUSIONES

ISACA Barcelona Chapter

1

El proceso de digitalización está transformando el mercado de auditoría. Entre las principales motivaciones para su utilización destacan el incremento de calidad y reducción de riesgos, la presión regulatoria, el volumen de información cada vez mayor a gestionar y la exigencia de los clientes de un mayor nivel de eficiencia.

2

Las firmas de auditoría están obligadas a aprovechar las nuevas tecnologías para su aplicación a los servicios que prestan. Las firmas están invirtiendo en el uso intensivo de tecnología, pues consideran que su nivel de madurez tecnológica es medio-bajo. Precisamente la necesidad de inversión y la adaptación al cambio son las principales barreras identificadas.

3

Se observa a nivel internacional la aparición de empresas especializadas en software y prestación de servicios orientados a la auditoría con la vocación de complementar las capacidades necesarias en los equipos de auditoría.

LA TRANSFORMACIÓN DIGITAL EN EL SECTOR DE LA AUDITORÍA

CONCLUSIONES

ISACA Barcelona Chapter

4

Para una adopción total de la tecnología es necesario reorientar el rol del auditor y el mix de habilidades que debe tener un equipo de auditoría. La adopción de nuevas tecnologías redundará en que se podrá dedicar más tiempo a la planificación y elaboración de conclusiones (en detrimento de la realización de pruebas), y los perfiles actuales de los profesionales de auditoría deberán evolucionar hacia un mayor nivel de conocimiento y capacidades tecnológicas.

5

Actualmente existe un abanico de tecnologías disponible muy amplio pero su aplicación a a la auditoría tiene grados de madurez muy diversos. Así, existen tecnologías con un grado de madurez muy alto como puede ser el caso de analytics, otras con un grado de madurez medio pero suficiente para considerar su aplicación, como puede ser el caso de la automatización de procesos y otras en un estado aún incipiente en el que se está experimentando para conocer su aplicación a la auditoría, como puede ser el caso del machine learning y la realidad virtual aumentada.

6

Las principales directrices del modelo de digitalización para la auditoría son: la estandarización de sistemas, la movilidad y la interconectividad de los equipos de auditoría, la colaboración entre los equipos y con los clientes, la automatización y eficiencia de los procesos, el análisis y visualización de la información disponible, la disponibilidad de la información y el cumplimiento regulatorio.

7

Las firmas de auditoría tienen que ponerse en marcha y adaptarse al nuevo entorno digital estableciendo su propia hoja de ruta a abordar en los próximos años, no sólo para maximizar su negocio, sino para garantizar su supervivencia. Dicha hoja de ruta, tal como se recoge en el propio estudio, dependerá tanto del tamaño de la firma como de su nivel de madurez tecnológica.

RISCOS A CONSIDERAR
Objectius i Abast

ISACA Barcelona Chapter

Objectiu	Conèixer els principals riscos que existeixen en el entorn com activitats de control rellevants i obtenir un conjunt de recomanacions per a millorar el nivell de control de la informació que es processa i es maneja, a partir de la revisió dels controls operatius i de gestió dels sistemes d'informació
Analitzar la situació actual	Anàlisi de seguretat cobrint l'estratègia, l'organització, els processos, la tecnologia i les persones per identificar les debilitats tant tècniques com organitzatives que puguin resultar en un impacte econòmic, d'imatge o legal per al negoci. Anàlisi de riscos, alineat amb negoci, que permeti proposar un pla de gestió determinant el nivell de risc acceptable per a l'organització.
Definir on vull anar	Definir un model de seguretat objectiu que inclogui tant un model d'organització com l'estat de seguretat objectiu en base al nivell de risc acceptable. Definir un pla d'acció de projectes de seguretat, organitzats temporalment i prioritzat sobre la base del cost, esforç i benefici de la implantació. Avaluar el risc que tindria la no execució dels mateixos

RISCOS A CONSIDERAR
Alguns riscos identificats

ISACA Barcelona Chapter

RISC	Descripció del Risc
R01	Accés no autoritzat mitjançant atacs i fuga d'informació a causa de la inexistència d'una política de contrasenyes, per la manca de polítiques de gestió d'usuaris i segregació de funcions.
R02	Accés malintencionat a la informació sensible (RRHH, expedients, instal·lacions crítiques, ...) causada per ciberatacs que exploten les vulnerabilitats existents en l'entorn de les TI.
R03	Pèrdua d'integritat d'informació sensible pel fet que alguns sistemes TI són vulnerables i/o la manca de mecanismes de detecció i resposta a atacs.
R04	Bretxa d'informació sensible (clients, empleats, expedients, bases de dades ...) a causa d'una manca de política clara i actualitzada, per falta de classificació de la informació que deriva en un mal tractament de la mateixa (nivell de conscienciació millorable) o que no es disposa d'eines adequades per protegir aquesta informació (xifrat, marques d'origen, registres esquer ...)
R05	Existència de sistemes i aplicacions vulnerables que suporten processos crítics causat per una deficiència de control o per una insuficient integració de seguretat
R06	Interrupcions de sistemes crítics causades per una infecció malware o un ciberatac.
R07	Indisponiblitat de sistemes crítics a causa de falta de Pla de Continuïtat de Negoci i incapacitat de recuperació per falta de procediments i/o eines.
R08	Incompliment legal per falta de seguretat en el disseny per nous sistemes / projectes i absència de classificació i tractament d'informació.
R09	Augment de l'impacte empresarial a causa de la manca d'eines i mecanismes per a la detecció i resposta d'incidents de Seguretat TI.
R10	Dependència de proveïdors externs en activitats clau sense revisió de seguretat que afecten a operacions

RISCOS A CONSIDERAR
Principals polítiques aplicables

ISACA Barcelona Chapter

POL	Descripció de la Política
P01	Gestió d'actius
P02	Polítiques de seguretat.
P03	Organització de la seguretat de la informació
P04	Seguretat relacionada amb Recursos Humans
P05	Control d'accessos
P06	Seguretat física i ambiental
P07	Seguretat operativa
P08	Seguretat de les comunicacions
P09	Xifrat i signatura electrònica
P10	Relació amb proveïdors
P11	Adquisició, desenvolupament i manteniment dels sistemes d'informació
P12	Gestió d'incidents
P13	Gestió de la continuïtat del negoci
P14	Compliment legal, regulacions i auditories

ISACA®

Barcelona Chapter

??????

ISACA®
Barcelona Chapter

GRÀCIES

joaquim.altafaja@isacabcn.org